STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

A U.S. GOVERNMENT INTERAGENCY STRUCTURE TO COMBAT TERRORISM

BY

LIEUTENANT COLONEL GEORGE J. WOODS, III
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

A U.S. Government Interagency Structure to Combat Terrorism

by

George J. Woods, III
U.S. Army

Professor Frank Jones
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel George J. Woods, III

TITLE: A U.S. Government Interagency Structure to Combat Terrorism
FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 26 CLASSIFICATION: Unclassified

Terrorists viciously attacked us on 11 September 2001 killing thousands of Americans. Terrorists supported cells located throughout the world, including within the US, executed these attacks and caught the United States by complete surprise. Terrorist acts have grown in frequency and audacity over the years but these attacks threaten our most critical national interest – our citizens' welfare and our homeland.

The President must organize the United States for a sustained war on terrorism. The US must attack terrorists where they live and protect the American homeland from them as well. It is not a fight that one US government agency can win by itself. Our current national security structure has not kept pace to deal with new terrorist organizations. The recent attacks demonstrate the need to re-examine our national security system and make needed changes to prevent similar terrorist attacks. There is no one right answer that absolutely guarantees their prevention but we must act to eliminate deficiencies when they are discovered. The purpose of this paper is to examine the current situation terrorism presents, assess our current preparedness to deal with this problem and recommend organizational interagency structural changes required to sustain a prolonged war to defeat international terrorism.

TABLE OF CONTENTS

A US GOVERNMENT INTERAGENCY STRUCTURE TO COMBAT TRANSNATIONAL TERRORISM

Terrorists viciously attacked the United States on 11 September 2001 killing thousands of Americans and several hundred foreign workers in near-simultaneous attacks on the World Trade Center and the Pentagon. Another forty Americans died in Pennsylvania when they took action against the terrorists aboard United Airlines Flight 93 that was destined for an unknown target that would have caused even more deaths. Nineteen terrorists supported by an unknown number of cells secretively planned and executed these attacks for several months, maybe even years, and caught the United States government, the intelligence community, law enforcement agencies and the American people by complete surprise. Acts of terrorism are not new. Over the past twenty years they have been growing in frequency and audacity, but these attacks have clearly awakened the American people, convincing them that the United States' most critical national interest – the welfare of its citizens and its homeland – is threatened by this cunning and vicious foe.

Since these events, the Bush administration has reacted quickly to the crisis, garnering international cooperation and making initial headway in defeating Usama Bin Laden's network of Al Qaeda terrorists. However, President Bush has said on numerous occasions that this is not going to be a short war on terrorism. As much as initial actions have made significant progress in disrupting Bin Laden's network to date, the President must organize the United States for a sustained war on international terrorism. The US must attack the terrorist networks where they live, while protecting the American homeland from terrorists ready to attack from within its borders. Fighting terrorism is a complex matter. It is not a fight that can be delegated to one agency of the United States government and be reasonably assured of success. It is a fight that will require the focused efforts of numerous federal agencies to defeat this current threat.[1]

Our current national security structure based on the National Security Act of 1947 was enacted for the purpose of coordinating national security strategy to defeat the nuclear threat the Soviet Union posed during the Cold War. It is a system that has expanded to handle a variety of broad and highly complex national security issues. Nonetheless, the world has changed dramatically and the US national security structure has not kept pace to deal with the emerging threats to our security. Clearly the recent attacks demonstrate the need to re-examine how our national security system is structured relative to this new threat and make needed changes to prevent more Americans from perishing at the terrorists' hands. There is no one right answer that guarantees the prevention of any more terrorists attacks on the US but we must act to eliminate deficiencies when they are discovered. The purpose of this paper is to examine the current situation terrorism presents, assess our current preparedness to deal with this problem and recommend organizational interagency structural changes required to sustain a prolonged war to defeat international terrorism.

THE ENVIRONMENT - TERRORISM

To find solutions to the problem, we have to define the terrorist threat and its components. The following questions must be asked and answered. What is the nature of the terrorist threat against the United States? How have modern terrorists adapted in this changed world? How are these changes different in practice – the introduction of networks and netwar? These questions must be addressed before our national security systems can reorganize to defeat them.

WHAT IS THE NATURE OF THE TERRORIST THREAT AGAINST THE UNITED STATES?

Terrorism is "the process of using terror, violence, and intimidation to achieve an end."[2] In more recent articles this definition has been more clearly linked it to a political agenda by defining terrorism as "politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents."[3] Gregory Copley takes exception to this definition because he believes that terrorism can "infuse military as well as civilian targets; terror can paralyze or distort the minds of professional leaders as well as the minds of 'innocent bystanders'."[4] International or transnational terrorism is the conduct of terrorist acts that span national borders and are committed against nation's facilities or people abroad such as embassies; ships, bases or aircraft; and citizens travelling or stationed internationally.[5] They can also be acts committed on a country's homeland like those that occurred against the World Trade Center and the Pentagon.

The United States is the sole "super" power that survived the Cold War. Its global reach and influence have grown while other nations in the world have struggled with regional instability as nations redefine themselves in terms of their interests, objectives and internal forms of government to achieve those objectives. Meanwhile, the US and particularly its military, although smaller in size, has grown in global capability across the entire spectrum of war – from low intensity conflicts to major theater war. The Gulf War and other conflicts over the past decade have shown the relative impotence of other nations to oppose the United States militarily or by any other instrument of national power. Since *states* (nations) with opposing agendas have been unable to influence United States policy and interests, *non-state organizations* have emerged in their place to oppose US policy and well recognize they must use asymmetric warfare to succeed in hurting the US.

HOW HAVE MODERN TERRORISTS ADAPTED IN THIS CHANGED WORLD?

These non-state organizations, including terrorist organizations, are not by themselves capable of directly defeating the United States' instruments of power with similar means (symmetrically); therefore, they have had to adopt other strategies to disrupt systems or influence the lessen our political will. Transnational terrorists have several options. They can appeal to the rest of the world as a weapon used on behalf of the weak attacking nation states asymmetrically (attacking means with unlike means). They can use media-grabbing terrorist acts to assert their identity, command attention and damage the reputation of the nations they attack. They may also use terrorism as a strategy to destroy the current world political structure for the purpose of creating a new order.[6] With the United States being the strategic center of gravity for world democracy and global trade, their aim is increasingly directed towards US targets. Their purpose is to create enough fear, destruction and disruption to defeat the American will to continue to prosecute policies that oppose the terrorists' objectives, whether those objectives are political or religious ones. And what better way to terrorize and discredit the powerful world leader than to attack targets within its own borders killing thousands of its own people with "weapons" (fuel-filled commercial aircraft) made within the United States itself?

But to prosecute this asymmetric strategy terrorist organizations have had to adapt. They have increasingly become more amorphous and less hierarchical. They are more likely inspired by religious or ideological agendas. Technology and the information age have enabled terrorist organizations to be more decentralized as well as more effective and lethal. Sharing information has enabled them to coordinate activities and learn the lessons from successful terrorist acts as well as unsuccessful acts. Cell phones and the Internet are key technological enablers for them. These technological enablers have also allowed the organizations to grow larger admitting more "amateur" terrorists – terrorists with less training. These amateurs attain the level of knowledge they need to operate and build weapons. Weapons have become simpler to build and are more frequently composed of legal products purchased commercially, such as fertilizer.

In order to survive to move to their targets and achieve surprise, terrorist organizations must remain invisible and undetected to authorities and law enforcement agencies. Yet they must be able to congregate to train, prepare and gather the resources they need. Further, for the most part, terrorists still need support from state-sponsors to provide these resources to train, sustain and operate their organizations.[7] State sponsorship tends to increase their effectiveness and reach. Terrorist organizations with accessible resources increase their technical and tactical capabilities. State-sponsored terrorists have an increased chance of developing the technical knowledge and materials to build weapons of mass destruction such as nuclear, biological or chemical bombs. They have increased technological means to share this knowledge and develop new tactics for employing these weapons in a secure environment. Therefore, they are better trained, better equipped, harder to detect and deadlier. Network-centric strategists have given their strategy and tactics a name – netwar.

HOW ARE THESE CHANGES DIFFERENT IN PRACTICE – THE INTRODUCTION OF NETWORKS AND NETWAR?

Arquilla and Ronfeldt, network-centric advocates working for RAND, define netwar as an:

> "emerging mode of conflict (and crime) at societal levels, involving measures short of war, in which the protagonists use – indeed, depend on using – network forms of organization, doctrine, strategy, and communication. These protagonists generally consist of dispersed, often small groups who agree to communicate, coordinate and act in an internetted manner, often without a precise central leadership or headquarters... It differs from traditional modes of conflict and crime in which the protagonists prefer to use hierarchical organizations, doctrines, and strategies as in the past efforts to foster large, centralized mass movements."8

The revolution of technology in the information age has enabled this new form of warfare to develop. Arquilla and Ronfeldt further describe how networked organizations remain widely dispersed and secretive while seeking targets to act upon. Then, once identified and targeted, the netwarriors attack stealthily from multiple approaches to "swarm" against their target.[9]

Terrorists will become further diversified, decentralized and flexible in applying these techniques. They will rely on networks enabled by information age technology and will attempt to exploit weaknesses in US defenses.[10] Network cells will remain secure by their dispersion, assimilation into existing societies and virtual invisibility. Gaps created in US defenses such as those areas not covered by law enforcement agencies, the military, or other government agencies create the infiltration lanes and battlespace for these terrorists and those who support their operations. Terrorists will also seek support and assistance from other terrorist groups, failed states or international crime organizations for the resources they need to survive. Additionally, they will continue to exploit the seams created by the US government's lack of cohesive and integrated policy and structure to detect and arrest or attack these terrorist organizations. What do these shifts in tactics and strategies mean for US national security?

Arquilla and Ronfeldt listed several implications nation states must consider. First, hierarchically structured organizations have a difficult time fighting networked organizations. Hierarchical ones are too slow to locate and coordinate actions against netwarriors. Second, the authors believe networks must be used to defeat other networks. Adopting the principles of network structures is essential in defeating the terrorists' decentralized, agile capabilities. Finally, they conclude that the one who masters the network form first *and best* will gain a major advantage.[11] Our inability to detect and stop the terrorist networks became evident on 11 September. How is the United States government presently structured to handle networked terrorists and how must it adapt itself to defeat these netwarriors?

THE CURRENT US NATIONAL SECURITY STRUCTURE AND ISSUES.

CURRENT US STRATEGIC ORGANIZATION.

The United States governmental structure at the strategic level is derived from the National Security Act of 1947 as well as the Bush administration's own design before and in response to the attacks on 11 September. Shortly after assuming office in January 2001, President Bush published his National Security Presidential Directive One (NSPD-1) and organized his National Security Council. Their purpose is "to advise and assist the President in integrating all aspects of national security policy as it affects the United States - domestic, foreign, military, intelligence and economics *[in conjunction with the National Economic Council (NEC)].*" He stated that the NSC system is a "process to coordinate executive departments and agencies in the effective development and implementation of those national security policies."[12] He organized the council system around interagency meetings of Principals and Deputies where decisions could be made and issues resolved below the presidential level. Policy Coordination Committees (PCCs - i.e. interagency working groups), conduct the day-to-day interagency coordination and "shall provide policy analysis ... and ensure timely responses to decisions made by the President."[13]

As a result of the attacks on 11 September, the Bush administration took quick action to respond to the threat to US security. First, he appointed former Governor Tom Ridge to a cabinet level position. As the first-ever Director of Homeland Security (also known as the Assistant to the President for Homeland Security), Governor Ridge had to advise President Bush on the creation of a completely new organization. Homeland security requires coordinating the activities of more than 70 agencies within the United States federal government.[14] Coupled with the state and local agencies that would respond first in subsequent attacks on the US and the numerous agencies required to prevent these attacks from occurring again, the task has proven to be a daunting one. Second, the administration looked at the NSC system for handling national security issues as a template for a brand new Homeland Security Council (HSC) system. On 29 October 2001, President Bush issued his first Homeland Security Presidential Directive (HSPD-1). This document, like NSPD-1, created an HSC system similar to the NSC system structure to "ensure the coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies."[15] Additionally, he created two new positions. For protection of information systems, the President appointed a Special Adviser to the President for Cyber-security and to coordinate and integrate all other counterterrorism-related actions he appointed a Deputy National Security Advisor for Counterterrorism. Both advisors report to the National Security Adviser and the Homeland Security Director to integrate all national security actions to combat terrorism.[16] Between the NSC and HSC systems, an integrated national security strategy is supposed to emerge, but it has not. Instead, he has established duplicate and competing systems.

This lack of integration and competing interagency processes stemming from the President's directives create, at the strategic level, the battlespace Arquilla and Ronfeldt discuss in their netwar analysis. As Frank Hoffman, a member of the Hart-Rudman commission, aptly states,

> "...the Bush administration has taken a different tack. The implication is that Ridge will coordinate domestic security, while Dr. Condoleeza Rice and the NSC continue to focus on foreign policy, international relations and defense. It is difficult to see how a comprehensive national security strategy that incorporates the various components relevant to homeland security - nonproliferation, threat reduction, diplomatic efforts to limit terrorism, intelligence, special operations, law enforcement, border security, and economic interests - is going to be produced. *The administration divorced the defensive side of homeland security from the international dimension potentially confounding security priorities, confusing accountability and diffusing responsibility.* The NSC and HSC have competing staffs, with overlapping responsibilities for directing intelligence, contingency planning, exercises and investments that contribute to homeland security. (italics added)"[17]

Furthermore, the placement of the Counterterrorism and Cybersecurity advisers within the structures further confuses the lines of responsibilities. Hence, at the strategic level, US national security solutions intent on combating terrorist networks begin to breakdown. Furthermore, the problem is exacerbated by our reliance on traditional bureaucratic and hierarchical systems in our executive branch of government. This structure developed over time and has established a proven track record that helped make the United States the global power it is today. However, this structure requires adaptation to defeat the networked terrorist threat.

BUREAUCRACIES AND HIERARCHICAL ORGANIZATIONS.

Although not ideal for combating new terrorist organizations, bureaucracies and hierarchical organizations are not completely without merit in determining foreign policy or recommending national security decisions. First, bureaucracies entail the division of labor that provides for organizing and assigning tasks. This, in turn, creates experts within those assigned fields. Second, competing organizations with different tasks ensure that different ideas or perspectives are considered in the decision making process (at least theoretically). Third, they provide for clear lines of responsibility and chains of command to govern the execution of tasks. Fourth, rules and standard operating procedures exist to regulate and govern behavior of large organizations. Fifth, written records document the bureaucracies' activities. Sixth, personnel within these organizations are compensated and promoted allowing the "best and the brightest" within their fields to rise to the top of the organizational ladder. Finally, with expertise massed in these organizations conditions exist to promote proactive planning – the anticipation of events rather than merely reacting to events that happen.[18] These characteristics describe the "*theoretical* basis for the view that bureaucracies contribute to the rational decision-making"[19] process. Some of these benefits organizations *actually* experience in practice as well. But Kegley and Wittkopf describe the negative side to hierarchical bureaucracies that many organizations including the US government experience day-to-day in the way they deal with each other and how they shape the behavior of the people within their organizations.

They describe organizations that exhibit parochial behavior promoting their self-interests and placing them before national interests. They also describe bureaucracies as competitive organizations vying for resources and decisions that favor their own agenda. These organizations seeking more resources and acting out of self-interest also seek to expand their roles in order to establish their importance and value. Bigger budgets, expanded roles and missions usually translate into larger organizations that wield more power and promote their long-term survival. Bureaucracies develop cultures centered on accomplishing their mission but also preserving their existence and influence. Many of these behaviors manifest themselves in organizational cultures that promote exclusiveness and secrecy, conformity among its members, deference to convention and reliance upon traditional solutions to solve new problems. Consequently, these factors combine to create bureaucratic organizations that, in practice, resist change, compete outright with other governmental organizations, and sometimes, willingly commit "bureaucratic sabotage" of Presidential decisions.[20]

Somewhere between the extremes of the theoretical organizations and those in practice that Kegley and Wittkopf describe is the "ideal" bureaucratic organization that needs to be developed to ensure US security and well-being, both domestically and abroad. Key to organizing the US national security structure for the purpose of protecting itself from future attacks will be to harness the advantages of "theoretical" bureaucratic organizations and minimizing the disadvantages described in "practicing" bureaucratic structures. It will be necessary to restructure the US government's interagency bureaucracy to avoid traditional solutions to combating the new terrorist threat and to ensure coordination and cooperation exists at all levels – from the strategic through the tactical level – to defeat terrorism. The reorganization should take advantage of institutional specialization that has proven its worth and developed a core of seasoned veterans. Further, these new structures must incorporate these experts and combine them with others to solve the new and very complex interagency problems the terrorists pose to US national security. Said another way,

> "...because their functions are different, military officers, spies, diplomats, and lawyers see problems and their solutions differently. No one of these different approaches is expendable. To succeed, the US government needs them all and needs vigorous advocates for each. The best way to increase interagency coordination will be the one that promotes coordination while respecting these differences and enhancing their forceful expression."[21]

Fixing the problem requires two major steps. First, clear definitions of roles and responsibilities must be assigned to existing hierarchical organizations to take advantage of their size, procedures and massed expertise. Second, interagency structures must be inserted throughout theses hierarchical organizations to create the interagency networks that will optimize the US government's ability to combat terrorist networks. These interagency networks will have to be established at all levels: strategic, operational and tactical to ensure that strategic objectives and policy are translated into tactical missions executed by operators at the grass roots level.

HOW SHOULD THE US GOVERNMENT ORGANIZE ITSELF FOR THE SUSTAINED FIGHT AGAINST TERRORISM?

DEFINING FUNCTIONS TO COMBAT TERRORISM

The fight against terrorism is a complex problem involving numerous agencies and departments at the national, state and local levels. It is both a domestic problem and an international one. To protect our national interests requires defense of the homeland and attacking the terrorist threat at its source. The first step in reorganizing the US government to achieve unity of effort is by establishing clear definitions of roles and responsibilities, then assigning them to organizations with "strategic" responsibilities. These organizations would be responsible for coordinating and integrating US strategic policy across multiple organizations to achieve the desired effect and successfully combat terrorism. Joint Doctrine helps us define the crucial functions involved in combating terrorism – the offensive and defensive ones.

Antiterrorism encompasses the defensive measures taken to protect America and Americans. These defensive measures aim to reduce vulnerability to terrorist acts by including training and other measures that balance the protection of assets with the mission, infrastructure and available manpower and resources.[22] Antiterrorism measures occur at home and abroad. These measures involve the protection of infrastructure, citizens and systems in the United States and those national assets abroad, most commonly US embassies and consulates, military installations and other facilities worldwide. Offensive measures taken to combat terrorism are called **Counterterrorism** measures. These measures prevent, deter and respond to terrorists' acts and occur within the United States and abroad. They include preemptive, retaliatory and rescue operations.[23] They can involve attacking terrorist cells located within the United States and attacking terrorist sanctuaries worldwide, such as those recently conducted in Afghanistan.

Two additional areas of importance help define roles and responsibilities. To defeat terrorism, we have to also consider the offensive and defensive components of informational warfare or cyber-warfare.[24] The US Army War College's Primer on Information Operations defines these aspects. It states that **Information Operations** are "...those actions taken to affect an adversary's information and information systems while defending one's own information and information systems. Information operations also include actions taken in a non-combat or ambiguous situation to protect one's own information and information systems as well as those taken to influence target information and information systems."[25] Information operations will have to be conducted internationally and within the United States. Information Operations, in the context of this paper, focus solely on the aspects of attacking and defending information systems and refer exclusively to cyber-security measures, not the full aspects of all information operations. Finally, the President defined **Incident Management**, one of the responsibilities that require policy and actions in order to respond to terrorist acts that could not be prevented. Again, terrorist incidents will occur within the United States and abroad. These measures, because they span various agencies, require one organization to define policy, devote resources and monitor policy execution. Keeping these four functions in mind, the next step is to assign responsibilities. **Table 1** proposes an alignment of responsibilities for functions required to combat terrorism and is further explained below.

NSA and NSC Staff - Coordinate/Advise President on Global War on Terrorism (GWOT)

	Antiterrorism (AT)	Counterterrorism (CT)	Incident Management (IM)	Information Ops
Within the USA	HLS (DoD lead agency)	HLS (DOJ lead agency)	HLS (FEMA lead agency)	CySA (DoJ lead agency)
External to USA	CTA (DoS lead agency)	CTA (DoD lead agency)	CTA (DoS lead agency)	CySA (DoD lead agency)

CTA – COUNTERRORISM ADVISER HLS – HOMELAND SECURITY ADVISER CYSA- CYBER SECURITY ADVISER

TABLE 1 FUNCTIONS AND ASSIGNMENT OF ROLES AND RESPONSIBILITIES.

ACHIEVING UNITY OF EFFORT AT THE STRATEGIC LEVEL.

First and foremost, the President should eliminate the dual structure currently in effect as a result of NSPD-1 and HSPD-1 and require a single organization and system rather than two with shared responsibility, which leaves the President as the arbitrator. Additionally, the President should expand the NSC's role to include homeland security. This will effectively assign all four functions required at the strategic level to conduct the global war on terrorism (GWOT) under one organization. The NSC would be responsible for advising the President on actions or policies to combat terrorism, establish objectives and priorities to meet requirements, and develop a coherent, integrated national security strategy intent on protecting America and eliminating the terrorist threat. The National Security Council and the NSC system are best suited for this responsibility because of the established interagency network and inherent presidential or strategic viewpoint the NSC system takes regarding national security issues.[26] Though it has its shortcomings, the NSC system has proven effective since 1947 with its well-established multi-agency connections and reputation for successfully managing national crises.

Next, the President should reassign the Homeland Security Adviser, the Cyber-security Adviser and the Counterterrorism Adviser to the NSC staff. These advisers would be responsible for coordinating, recommending and supervising strategic policy with regard to the functions shown in **Table 1**. The HLS adviser would be responsible for policies within the United States. The Counterterrorism adviser would be assigned responsibility for policy external to the US. The Cyber-security adviser would have responsibility for integrating both the domestic and international policies regarding cyber-security aspects of information operations since this area tends to span international borders.

The NSC staff is relatively small and would become ineffective if too large, yet the complexity of integrating policy on each of the four functions would overwhelm the existing structure. Therefore, within these assigned functions, the NSC would rely upon currently configured hierarchical organizations with sufficient staffing and traditional expertise to assist in coordinating, staffing and supervising policy decisions. They would also manage the resources and execute budget integration and supervision for those responsibilities. How might this concept look in practice?

ASSIGNMENT OF RESPONSIBILITIES

Antiterrorism measures would fall under the HLS adviser. He would coordinate with DoD, and its newly established Northern Command (as well as other Federal agencies), to plan, supervise and resource interagency activities. Specifically, these activities would be associated with defending our borders, protecting critical US infrastructure, ensuring the safety of US airspace, and directing national intelligence or law enforcement agencies to collect intelligence against terrorists entering the country or those already within it. Counterterrorism measures, on the other hand, would be the Department of Justice's (DoJ) responsibility under the HLS adviser since attacking terrorist cells within the United States has primarily been a law enforcement issue. Identifying terrorist activities and havens and arresting suspected terrorists before they act is a role for which the Federal Bureau of Investigation (FBI) and other law enforcement agencies at the local or community level are best suited. The HLS adviser would depend on the Federal Emergency Management Agency (FEMA) for its expertise in organizing, training and coordinating incident management measures. FEMA has evolved into an effective structure within the US for responding to natural disasters and minimizing the effects of natural disasters and other large-scale catastrophes.

External to the United States, the Counterterrorism adviser would have similar tasks coordinating and supervising strategic policy for the GWOT relying upon the Departments of Defense and State primarily as his supporting agencies for coordinating, supervising and resourcing functional activities overseas. For instance, the State Department would be responsible for antiterrorism and incident management measures overseas (except on military installations). Ambassadors and their country teams already exist to represent the United States' interests abroad for all US personnel and facilities located in numerous countries throughout the world. They would be responsible for measures, traditionally within their area of expertise, to protect US national interests abroad by hardening facilities to protect them from possible terrorist attacks. They would also be responsible for coordinating host-nation support efforts to respond to terrorist incidents that occur to US personnel or facilities countries where there is a US presence. They would establish policies to ensure the safety of US personnel abroad and coordinate with US and foreign intelligence and law enforcement agencies of the host countries to gather intelligence designed to identify and detect threats targeting US interests abroad. Attacking the sources of terrorism abroad would be a Department of Defense

(DoD) responsibility. The Defense establishment is ideally structured with the existing Joint Staff and regional combatant commanders (CINCs) to devise strategy and implement policy internationally to identify, detect, seek and destroy or neutralize sources of terrorism, either unilaterally or cooperation with other nations.

As stated earlier, Information Operations would come under the auspices of the Special Advisor to the President for Cyber-security as the lead for coordinating national policy regarding information operations security measures. For support, the Cyber-security adviser would rely on the Justice Department with its expertise in operating the National Infrastructure Protection Center (NIPC). The NIPC has been established within the Federal Bureau of Investigation and is charged with "developing information resources and working relationships with infrastructure owners and operators and providing a mechanism for information sharing between the public and private sectors. NIPC will develop all necessary assets and capabilities to support operations aimed at disrupting and defeating threats to critical infrastructures."[27] For Information Operations outside the US, DoD has already assigned SPACECOM responsibility for information operations within the military structure for both defensive and offensive measures.[28] SPACECOM has made significant progress in developing measures to protect information security and has developed the means of attacking threats through this medium. They are also a supporting command for the regional combatant commands worldwide and can leverage this existing relationship to integrate Information Operations into the established Department of Defense structure. This enhances integration of cyber-security policy and, with additional interagency assistance, should enable it to be broadened to include designing policy and developing measures to protect all governmental systems located overseas.

ESTABLISHING THE INTERAGENCY NETWORK FROM STRATEGIC TO THE TACTICAL LEVELS

Responsibilities for activities would be centrally coordinated and integrated at the NSC level with staff support and expertise from "lead agencies". However, none of these departments can do it all alone and accomplish the strategic goals without interagency support. Combating terrorism requires a "diplomatic component, a law enforcement component, an intelligence component, a financial component and a military component as well."[29] Network-centric advocates like Arquilla and Ronfeldt promote the concept that must be applied to the national security structure at all levels in order to eliminate the terrorists' freedom of movement, limit their battlespace and seize the initiative. Netwar advocates recommend using networks to combat networks. Several types can work; however, the most effective is the all-channel network. This type of network exists when all participants of a network or node are connected to each other. Although the most effective, they are also the most difficult to establish and to sustain.[30] They require robust, integrated packages of information-sharing technology to function effectively. They also require heavy investments in human capital. Robust information-sharing technology packages require people to use the equipment and make decisions to use the shared information.

Policy Coordination Committees established by the President's NSPD-1 are interagency structures by their nature and serve as the networked system as the strategic level. However, combining and reorganizing PCCs created by both national security and homeland security presidential directives will be necessary to achieve further efficiencies. Additionally, interagency operations centers should be established within appropriate executive branch departments to effectively coordinate and close the strategic level gaps within our current "stovepiped" system. Lastly, establishing interagency networks at the operational and tactical levels will be essential in order for the numerous departments to carry out interagency policy and translate strategic goals and objectives into operational and tactical missions conducted by interagency organizations at the lowest levels.

Applying an all-channel network structure to current forms within our governmental structure will be no easy task. Converting completely to a flat, decentralized and highly responsive structure that Arquilla and Ronfeldt suggest, especially in the midst of fighting the current war on terrorism, could be disastrous. Adding all-channel network structures to augment current hierarchical organizations rather than dismantle them and replace existing structures in the midst of the conflict is the optimal solution. In some cases, all-channel network principles are already being applied within current government organizations below the strategic level. In other cases, augmenting existing organizations can be done with relatively minor difficulty. How might the US apply some of these principles at the operational and tactical levels?

Use of interagency coordination groups and task forces could augment existing structures that will enable the current systems to adopt a networked structure to as part of the counter-netwar Arquilla and Ronfeldt describe. **Figure 1** graphically depicts a proposed structure for organizing the US government to combat terrorism. The depiction shows interagency operations cells (IOC), coordination groups (IACG) and interagency task forces (IATF) imposed on existing organizations and aligned functionally in accordance with **Table 1**. The structure depicts organizations at the strategic, operational and tactical levels. Interagency coordination groups would exist primarily at the operational levels while interagency task forces exist at the tactical levels to execute interagency operations in the form of an attack, an arrest or some other action requiring the coordination and synchronization of multiple agency actors.

The interagency coordination groups would provide expertise and advice to the commander or leader regarding capabilities that each organization can apply to assist in achieving desired operational objectives. They would provide policy recommendations and engage in planning for campaigns and major operations. Further, they would share information with and coordinate the support of their parent agency actors to achieve the interagency result desired. An example could be an interagency coordinating group working for a combatant commander. This group would consist of representatives from the Departments of Justice, State, Treasury, Commerce, Agriculture and the Central Intelligence Agency advising the commander and synchronizing the activities of their respective departments to identify, detect, target and destroy or arrest terrorists within a combatant commander's area of responsibility. They would also assist planners in establishing appropriate additional interagency organizations within an area of responsibility such as a subordinate unified or functional command or Joint Task Forces (JTFs).

Interagency task forces, on the other hand, would be interagency organizations that conduct tactical missions much like those that the Joint Interagency Task Force-East (JIATF-E) does in conducting counterdrug tasks in support of the SOUTHCOM area of responsibility. Their mission to conduct

> "detection, monitoring, and handoff of suspected drug trafficking events; coordinate counterdrug operations; conduct counterdrug engagement; and support Country Team and Participating Nation LEA initiatives to achieve an effective and coordinated multinational counterdrug effort in the US Southern Command Area of Responsibility."[31]

supports the nation's counterdrug strategy as an interagency organization. JIATF-E is an organization that is relatively permanent because of the sustained counterdrug effort the United States has been performing. Congressional directives and the 1994 National Interdiction Command and Control Plan established the Task Force. Since 1994, JIATF-East has made significant inroads not only in intercepting drugs smuggled into the United States, but also in developing a viable working interagency organization to serve as a model for other such undertakings. Over the years, the organization has developed bonds of trust and confidence among agency actors and the department chiefs they represent in developing effective interagency procedures that support achieving tactical and operational objectives in support of national strategy.[32] One could reasonably assume that similar organizations created in other regional combatant commands and organizations, whether they are coordinating groups or task

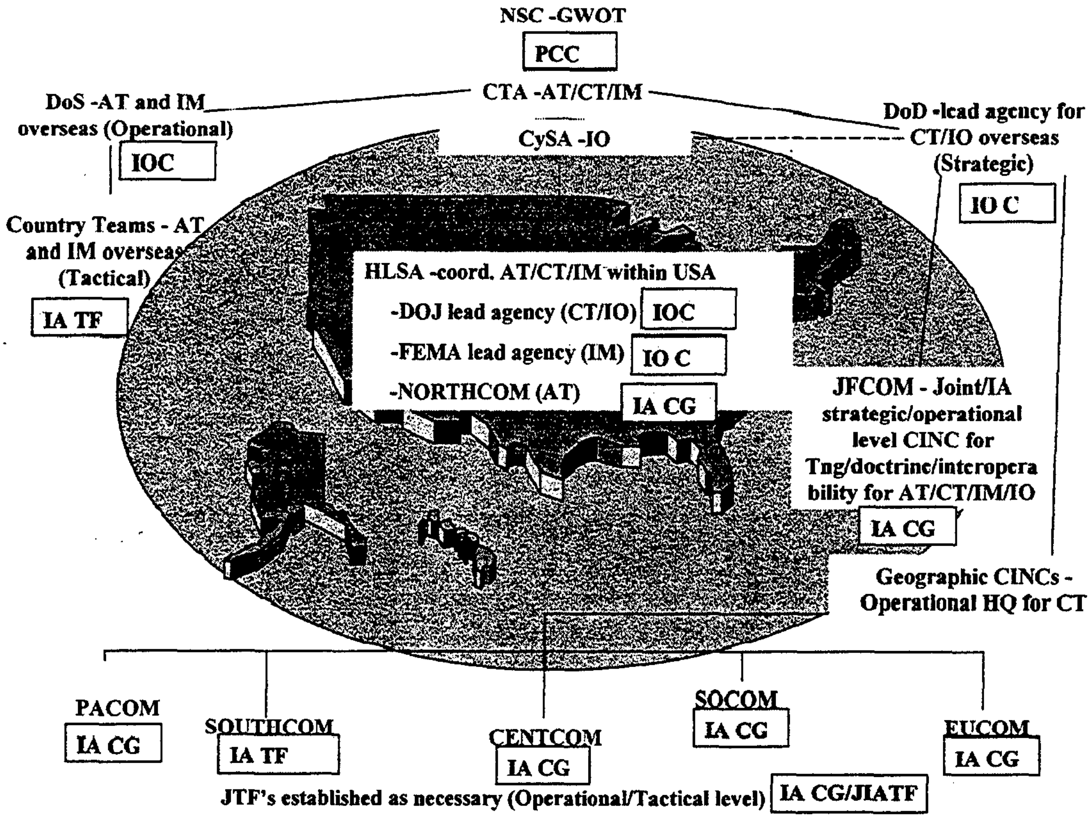
NSC -GWOT
PCC
CTA -AT/CT/IM
CySA -IO
DoS -AT and IM overseas (Operational)
IOC
DoD -lead agency for CT/IO overseas (Strategic)
IO C
Country Teams - AT and IM overseas (Tactical)
IA TF
HLSA -coord. AT/CT/IM within USA
-DOJ lead agency (CT/IO)
IOC
-FEMA lead agency (IM)
IO C
-NORTHCOM (AT)
IA CG
JFCOM - Joint/IA strategic/operational level CINC for Tng/doctrine/interoperability for AT/CT/IM/IO
IA CG
Geographic CINCs - Operational HQ for CT
PACOM
IA CG
SOUTHCOM
IA TF
CENTCOM
IA CG
SOCOM
IA CG
EUCOM
IA CG
JTF's established as necessary (Operational/Tactical level)
IA CG/JIATF

FIGURE 1 A U.S. GOVERNMENT INTERAGENCY STRUCTURE TO COMBAT TERRORISM

forces, will have the same success in overcoming parochial departmental agendas to achieve national interests rather than self-promoting ones.

Figure 2 depicts how the interagency structure would interconnect consistent with the requirements to conduct counter-netwar activities to defeat the terrorists. Shared information networks and databases would have to be created to speed the exchange of information and establish the all-channel network that Arquilla and Ronfeldt describe. The all-channel interconnectivity this augmentation offers will leverage the strength of existing traditional hierarchical structures while establishing the interagency coordination and action required to identify, find and take action against terrorists before they act or minimize the effect of their actions with rapid incident response. In effect, with structures in place to effect interagency coordination and action, the battlespace and freedom of movement enjoyed by terrorists today will shrink and further restrict their options. But structures alone are insufficient to ensure success. Procedural practices must be established to create a common language among multiple organizational cultures to aid in effectively and rapidly assigning tasks and defining priorities.

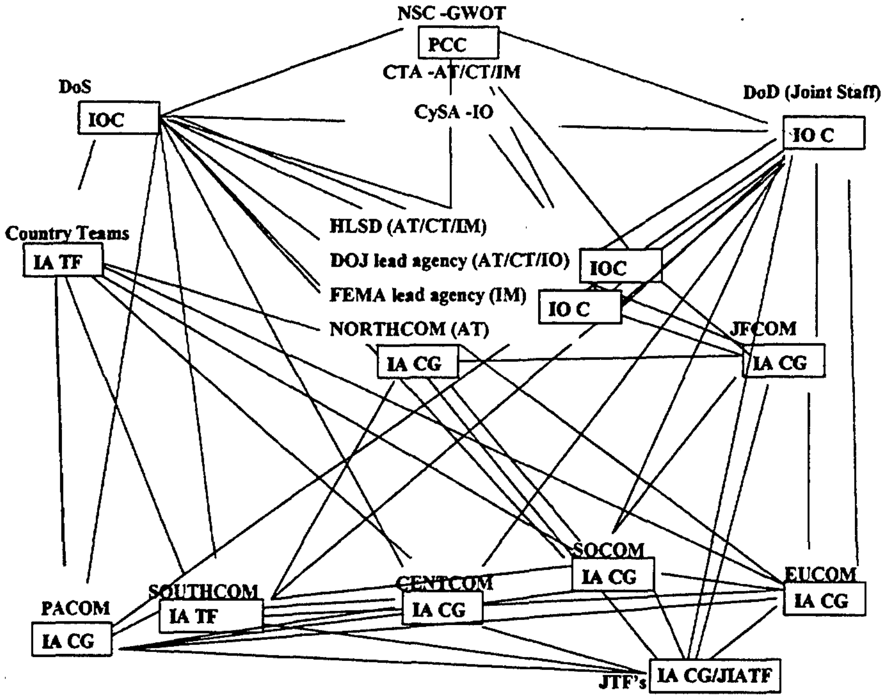

FIGURE 2 AN INTERAGENCY ALL CHANNEL NETWORK

PROCEDURAL CHANGES REQUIRED

At the strategic level, the National Security Council should develop procedures that dictate how the interagency process should work.[33] Although not a panacea, Presidential Decision Directive (PDD) 56 that served as the Clinton administration's process for conducting complex contingency operations, could serve as a starting point. Admittedly an imperfect process for conducting interagency operations at the strategic level, it does have its advantages. PDD-56 provided a framework and planning tools under the auspices of an executive committee answerable to the NSC Deputies Committee's supervision. The framework also provided for a fully integrated political-military plan that, in theory, synchronized all elements of national power in complex interagency contingency operations. Additionally, rehearsals, after action reviews and training became standard practices in conducting contingency operations. One report cited the combination of these practices showed a significant improvement in interagency effectiveness.[34] However, it had drawbacks as well.

Not all aspects the framework called for manifested itself in execution. One study identified areas where improvement could be made to enhance the effectiveness of PDD-56. First, PDD-56 was best suited for the strategic level. When applied below that level it ceased to be effective. Second, it functioned best with a strong leader who championed the process.

Third, the framework needed to provide for more flexibility in the plan to achieve versatility and acceptability. Finally, to be effective PDD-56 required dedicated funding to support training.[35] Using this analysis and developing procedures that the agencies can agree upon while leveraging the advantages of PDD-56 and minimizing it drawbacks is useful. It increases the probability that the NSC staff can develop an effective framework to energize and focus interagency planning to synchronize all elements of national power into a coherent, integrated strategy to prosecute the global war on terrorism. Since PDD-56 did not apply well below the strategic level what about the operational and tactical levels?

The Joint Staff has recently developed a generic political-military plan template that lists the key components of an interagency plan for contingency operations. Both PDD-56 and the generic plan focus primarily on humanitarian assistance operations or peacekeeping operations. However, these plans can easily be applied to operations to combat terrorism since interagency unity of effort is the desired outcome. To complete the development of the standardized interagency doctrine and interoperability procedures, the NSC should task the Department of Defense with this responsibility. Joint Forces Command (JFCOM) in Norfolk, Virginia (previously known as LANTCOM and ACOM) has already been assigned as the Department of Defense's headquarters for capturing joint lessons learned, conducting joint exercises and training, assessing joint interoperability and publishing joint doctrine. This headquarters could steadily adapt itself to an interagency perspective with augmentation from the various departments creating an interagency cell. Initiatives along these lines are already underway. *Millennium Challenge 2002*, an interagency exercise, is planned for April 2002 with the goal of assessing and improving interagency operations at the operational level.[36] The JFCOM cell should consist of senior representatives from the various departments who have had operational experience serving on either an interagency task force or an interagency coordination group. With experienced augmentation, JFCOM would better be able to execute the assigned role of creating interagency doctrine at the operational and tactical level.

CONCLUSION

This paper analyzed the current status of the interagency system and processes vis-a-vis the current terrorist threat. It identified how new terrorist organizations are different. It described as well how their organizational structures take advantage of traditional US hierarchical structures. Finally, it proposed a potential method of defining the problem and organizing the US governmental structure to respond to this new threat. The proposal recommends organizational concept using networks to combine the traditional strengths of existing departmental expertise within the US government with the advantages of interagency cells to enhance connectivity and coordination. This concept is designed to deal with the interagency complexity of operations we confront as well as sustain the long-term US effort to conduct the global war on terrorism. By no means a perfect or easy solution, it provides a realistic option to consider for organizing the US government's response to international terrorism with the ultimate goal of achieving unity of effort in defeating transnational terrorists that threaten the globe while protecting America's homeland and its citizens.

Word Count = 6,616

ENDNOTES

[1] Ivo Daalder and I.M. Destler, "Organizing for Homeland Security", Statement Before the Committee on Governmental Affairs, United States Senate, October 12, 2001. Internet site http://www.brook.edu/views/testimony/daalder/20011112.htm.

[2] William Morris, ed. American Heritage Dictionary (Boston, MA: Houghton Mifflin Company, 1976), p. 1330.

[3] Raphael F. Perl, "Terrorism, The Future, and U.S. Foreign Policy" (Washington, DC: Congressional Research Service, Library of Congress, September 2001), p. 3.

[4] Gregory Copley, "Defining Terrorism", Defense and Foreign Affairs Strategic Policy, Vol. 29, No. 10, November 6, 2001, p. 4.

[5] Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, Countering the New Terrorism (Santa Monica, CA: Rand Project Air Force, 1999), p xii.

[6] Ibid., p. 39-40.

[7] Ibid., p. 15.

[8] John Arquilla and David Ronfeldt, The Advent of Netwar (Santa Monica, CA: Rand, 1996), p. 5.

[9] John Arquilla and David Ronfeldt, Swarming and the Future of Conflict (Santa Monica, CA: Rand National Defense Research Institute, 2000), p. 5.

[10] Arquilla and Ronfeldt, in Countering the New Terrorism, p 54.

[11] Ibid, pp. 47-55.

[12] George W. Bush, "National Security Presidential Directive Number 1: Organization of the National Security Council System," (Washington, DC: The White House, February 13, 2001), p. 2.

[13] Ibid., p. 4. The regional committees include: Europe and Eurasia, Western Hemisphere, East Asia, South Asia, Near East and East Africa, and Africa. The eleven functional committees include: 1) Democracy, Human Rights and International Operations (Assistant to the President for National Security Affairs being the lead); 2) International development and Humanitarian Assistance (led by the Secretary of State); 3) Global Environment (co-led by the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy); 4) International Finance (led by the Secretary of the Treasury); 5) Transnational Economic Issues (led by the Assistant to the President for Economic Policy); 6) Counter-Terrorism and National Preparedness (led by the Assistant to the President for National Security Affairs); 7) Defense Strategy, Force Structure, and Planning (led by the Secretary of Defense); 8) Army Control (led by the Assistant to the President for National Security Affairs); 9) Proliferation, Counterproliferation, and Homeland Defense (led by the Assistant to the President for National Security Affairs); 10) Intelligence and Counterintelligence (led by the Assistant to the President for National Security Affairs); 11) Records Access and Information Security (led by the Assistant to the President for National Security Affairs).

[14] Daalder and Destler, "Organizing for Homeland Security".

[15] George W. Bush, "Homeland Security Presidential Directive Number 1: Organization and Operation of the Homeland Security Council," (Washington, DC: The White House, October 29, 2001), p. 1.

[16] The White House. "New Counter-Terrorism and CyberSpace Security Positions Announced" (Washington, DC: Office of the Press Secretary. Official Press Release, October 9, 2001), The White House Internet site: http://www.whitehouse.gov.

[17] Frank G. Hoffman, "Homeland Security: Impossible?" Proceedings (Annapolis, MD: US Naval Institute, Nov 2001), pp. 40-41.

[18] Charles Kegley and Eugene R. Wittkopf, "The Process of Decision Making: Roles, Rationality and the Impact of Bureaucratic Organization" American Foreign Policy. (New York: St. Martin's Press, 1996), pp. 475-476.

[19] Ibid., p. 476.

[20] Ibid, pp. 477-488.

[21] David Tucker, "The RMA and the Interagency: Knowledge and Speed vs. Ignorance and Sloth?" Parameters, 30 (Autumn 2000), p. 71.

[22] Department of Defense. Joint Doctrine for Military Operations Other Than War. Joint Publication 3-07 (Washington, D.C.: U.S. Joint Staff, 16 June 1995), p. III-2.

[23] Ibid.

[24] Bush, HSPD-1, p.1. The President established the position of Special Advisor for Cyber Security.

[25] The Army War College. Information Operations Primer, Course Four CD-ROM entitled Implementing National Military Strategy, (Carlisle Barracks, PA: U.S. Army War College, Academic Year 2001-2002), p. 2.

[26] Christopher C. Shoemaker, The NSC Staff: Counseling the Council (Boulder, CO: Westview Press, February 1991), p. 43.

[27] Department of Justice, Strategic Plan 2001-2006, found at Internet site http://www.usdoj.gov/05publications/05_04.html.

[28] The ideas in this paragraph are based on remarks made by a speaker participating in the Commandant Lecture's Series.

[29] White House Press Release, 9 October 2001.

[30] Arquilla and Ronfeldt, in Countering the New Terrorism, p. 49.

[31] Joint Interagency Task Force – East unclassified briefing comparing and contrasting the counter-drug and counter-terrorism and related interagency issues.

[32] Conversations with a former JIATF-E operator.

[33] Edward J. Filiberti, "National Strategic Guidance: Do We Need a Standard Format?" Parameters, 25, (Autumn 1995), p. 2. Filiberti says that the interagency coordination at the strategic level is a White House responsibility which therefore falls on the NSC to develop.

[34] National Defense University, "Improving the Utility of Presidential Decision Directive 56 – A Plan of Action for the Chairman of the Joint Chiefs of Staff" Institute for National Strategic Studies pp. I, 16-19.

[35] Ibid. pp. I, 16-19.

[36] Joint Forces Command, "Improving US Interagency Operational Planning and Coordination", White Paper Version 1.0, January 2001.

BIBLIOGRAPHY

Arquilla, John and Ronfeldt, David. Swarming and the Future of Conflict. Santa Monica, CA: Rand National Defense Research Institute, 2000.

Arquilla, John and Ronfeldt, David. The Advent of Netwar. Santa Monica, CA: Rand, 1996.

Bush, George W. "Homeland Security Presidential Directive Number 1: Organization and Operation of the Homeland Security Council," Washington, DC: The White House, October 29, 2001.

Bush, George W. "Homeland Security Presidential Directive Number 2: Combatting Terrorism Through Immigration Policies," Washington, DC: The White House, October 29, 2001.

Bush, George W. "National Security Presidential Directive Number 1: Organization of the National Security Council System," Washington, DC: The White House, February 13, 2001.

Carter, Ashton B. and Perry, William J. "Countering Asymmetric Threats" in Keeping the Edge, Managing Defense for the Future. Cambridge, MA: Preventive Defense Project, MIT Press, 2000.

Carter, Ashton B. and White, John P. Editors. Keeping the Edge, Managing Defense for the Future. Cambridge, MA: Preventive Defense Project, MIT Press, 2000.

Conversation with Joint Interagency Task Force – East member, Interview by author, 4 March 2002.

Conversations with several senior government officials from the NSC staff, State Department and the Central Intelligence Agency, Interview by author, 5 through 9 March 2002.

Copley, Gregory R. "Defining Terrorism". Alexandria, VA: Defense and Foreign Affairs Strategic Policy. Vol. 29, No. 10. 6 November 2001.

Daalder, Ivo H. and Destler, I.M. "A New NSC for a New Administration". Policy Brief Number 68 – November 2000. Brookings Institute Internet site: http://www.brook.edu/comm/policybriefs/pb068/pb68.htm.

Daalder, Ivo H. and Destler, I.M. "Organizing for Homeland Security". Statement before the Committee on Governmental Affairs, United States Senate, October 12, 2001. Brookings Institute Internet site: http://www.brook.edu/views/testimony/daalder/20011012.htm.

Davis, M. Thomas. "Homeland Security: New Mission of a New Century". Washington, DC: Northrup Grumman Analysis Center Papers, January 2002.

Decker, Raymond J. "Combating Terrorism: Observation on Options to Improve the Federal Response". Washington, DC: Testimony before the U.S. House of Representatives, April 24, 2001.

Department of Justice, Strategic Plan 2001-2006, found at Internet site http://www.usdoj.gov/05publications/05_04.html.

Department of National Security and Strategy. “The Interagency Process from Peace to War”. Carlisle Barracks, PA: U.S. Army War College, 1999.

Deutch, John, Kanter, Amold, and Scowcroft, Brent. “Strengthening the National Security Interagency Process” in Keeping the Edge, Managing Defense for the Future. Cambridge, MA: Preventive Defense Project, MIT Press, 2000.

Filiberti, Edward J. “National Strategic Guidance: Do We Need a Standard Format?” Carlisle Barracks, PA: Parameters, Vol. XXV, No. 3, Autumn 1995.

Hoffman , Bruce. “Responding to Terrorism Across the Technological Spectrum”. Carlisle Barracks: Strategic Studies Institute, United States Army War College, 15 July 1994.

Hoffman , Bruce. “Responding to Terrorism Across the Technological Spectrum”. Carlisle Barracks: Strategic Studies Institute, United States Army War College, 1994.

Hoffman, Frank G. “Homeland Security: Impossible?” Annapolis, MD: US Naval Institute. Proceedings, Nov 2001.

Hoover , Bruce. “Combatting Terrorism: A New National Strategy”. Carlisle Barracks: Strategic Studies Institute, United States Army War College, 7 April 1997.

Institute for National Strategic Studies. “Improving the Utility of Presidential Decision Directive 56: A Plan of Action for the Chairman of the Joint Chiefs of Staff”. Ft. McNair, Washington, DC: National Defense University, March 1999.

Joint Interagency Task Force – East unclassified briefing comparing and contrasting the counter-drug and counter-terrorism challenges and related interagency issues.

Kegley, Charles and Wittkopf, Eugene R. “The Process of Decision Making: Roles, Rationality and the Impact of Bureaucratic Organization” American Foreign Policy. New York: St. Martin’s Press, 1996.

Lesser, Ian O., Hoffman, Bruce, Arquilla, John, Ronfeldt, David, Zanini, Michele. Countering the New Terrorism. Santa Monica, CA: Rand Project Air Force, 1999.

Morris, William. Editor. The American Heritage Dictionary. Boston, MA. Houghton Mifflin Company, 1976.

National Defense University Planning Group. “Draft Generic Pol-Mil Plan”. Ft. McNair, Washington, DC: National Defense University, 1 September 2000.

Perl, Raphael F. “Terrorism, The Future, and U.S. Foreign Policy”. Washington, DC: Congressional Research Service, Library of Congress, September 2001.

Shoemaker, Christopher C. The NSC Staff: Counseling the Council. Boulder, CO: Westview Press, February 1991.

The White House. “Frequently Asked Questions About the War on Terrorism at Home and Abroad- What is Homeland Security?” Washington, DC: The White House Internet site: http://www.whitehouse.gov.

The White House. "Frequently Asked Questions About the War on Terrorism at Home and Abroad – What is the War on Terrorism?" Washington, DC: The White House Internet site: http://www.whitehouse.gov.

The White House. "History of the National Security Council 1947-1997". Washington, DC: The White House Internet site: http://www.whitehouse.gov.

The White House. "New Counter-Terrorism and CyberSpace Security Positions Announced" Washington, DC: Office of the Press Secretary. Official Press Release, October 9, 2001. The White House Internet site: http://www.whitehouse.gov.

The White House. "President Establishes Office of Homeland Security – Summary of the President's Executive Order The Office of Homeland Security and the Homeland Security Council" Washington, DC: The White House Internet site: http://www.whitehouse.gov, October 2001.

Tucker, David. "The RMA and the Interagency: Knowledge and Speed vs. Ignorance and Sloth?" Carlisle Barracks, PA: Parameters, Vol. XXX, No. 3, Autumn 2000.

U.S. Army War College. Information Operations Primer, Course Four CD-ROM entitled Implementing National Military Strategy, Carlisle Barracks, PA: U.S. Army War College, Academic Year 2001-2002.

U.S. Department of Defense. Joint Doctrine for Military Operations Other Than War. Joint Publication 3-07. Washington, D.C.: U.S. Joint Staff, 16 June 1995.